UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

JEWELL WEEKES, *on behalf of herself and all others similarly situated*,

Plaintiff,

v.

COHEN CLEARY, P.C.,

Defendant.

Case No.: 1:23-cv-10817-NMG

Judge Nathaniel M. Gorton

MEMORANDUM IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS PURSUANT TO FED. R. CIV. P 12(b)(6)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

I. INTRODUCTION

This case arises out of a cyberattack (the "Cyberattack") against Defendant Cohen Cleary P.C. ("Cohen Cleary" or "Defendant"), a law firm located out of Taunton, Massachusetts. Plaintiff Jewell Weekes ("Weekes" or "Plaintiff") is a former client of Cohen Cleary who claims that her personal identifying information and personal health information (collectively, "PII") was compromised as a result of the Cyberattack. She alleges that her compromised PII may have included her name, address, date of birth, Social Security number, medical information, and/or health insurance information. As a result, Plaintiff filed a Class Action Complaint (the "Complaint") against Cohen Cleary, asserting causes of action for: (1) negligence; (2) breach of confidence; (3) breach of implied contract; and (4) breach of implied covenant of good faith and fair dealing.

Plaintiff's Complaint fails to state a claim upon which relief may be granted. As set forth more fully below, Plaintiff's claim for negligence fails because she has not alleged the required breach and damages elements of her claim; her claim for breach of confidence fails because she fails to allege that Defendant affirmatively disclosed her PII; her claim for breach of implied contract fails because she does not allege the exchange of consideration, mutual assent, or cognizable damages; and her claim for breach of implied covenant of good faith and fair dealing fails because Massachusetts courts have held that such claims are duplicitous when a litigant also has raised a breach of contract claim. Consequently, Plaintiff's claims are fatally flawed and her Complaint should be dismissed in its entirety pursuant to Federal Rule of Civil Procedure 12(b)(6).

II. STATEMENT OF ALLEGED FACTS[1]

A. The Cyberattack

Cohen Cleary is a law firm that provides legal services in various areas of law, such as criminal law, family law, estate law, labor and employment law, consumer protection, and civil litigation, among others. (Compl. ¶ 14.) Plaintiff was a former client of Cohen Cleary. (*Id.* ¶ 7.) On or about September 30, 2022, Plaintiff alleges that Cohen Cleary discovered that it had fallen victim to the Cyberattack in which cyber criminals accessed Cohen Cleary's computer systems and accessed her PII. (*Id.* ¶¶ 3, 6.) Accordingly, Plaintiff now alleges that her PII, as well as "others similarly situated," were compromised as a result of the Cyberattack. (*Id.* ¶¶ 1-2.) That PII allegedly included her name, address, date of birth, Social Security number, medical information, and/or health insurance information. (*Id.* ¶ 1.) Plaintiff received notice of the Cyberattack from Cohen Cleary on or about November 23, 2022. (*Id.* at ¶ 3.)

Plaintiff does not allege how the Cyberattack occurred, nor does she identify any specific defect in Cohen Cleary's security systems, procedures, or training that may have contributed to it. Instead, she refers to certain security measures that can help reduce the risk of a cyberattack (*see id.* ¶¶ 26, 35-38), and goes on to broadly conclude that Defendant's security practices were deficient because of the mere occurrence of the Cyberattack. (*See id.* ¶ 50.)

B. Plaintiff's Alleged Harm

Plaintiff does not claim to have suffered any actual, pecuniary loss as a result of the Cyberattack. Instead, her alleged injuries are limited to:

- A "diminution in the value" of her PII, which Plaintiff recognizes is an "intangible property" (*id.* ¶ 12);

[1] These allegations are taken from the Complaint. Cohen Cleary accepts them as true for purposes of this Motion and reserves the right to dispute them later.

- Suffering "lost time, annoyance, interference, and inconvenience" as a result of the Cyberattack (*id.*);
- Suffering from "anxiety and increased concerns for the loss of privacy" associated with the possibility of cybercriminals utilizing her PII (*id.*); and
- The possibility of falling victim to fraud or identity theft as a result of a cybercriminal utilizing her PII (*see id.*).

Ultimately, and as the foregoing will demonstrate, Plaintiff's claimed injuries are not actual or cognizable, and thus, fail as a matter of law.

C. Plaintiff's Putative Classes, Causes of Action, and Prayer for Relief

Plaintiff seeks to represent two classes: a class of individuals whose PII may have been "exposed to unauthorized third parties" as a result of the Cyberattack (the "Nationwide Class"), and a subclass of all individuals within the State of Massachusetts" whose PII "was stored by Defendant and/or was exposed to unauthorized third parties" as a result of the Cyberattack (the "Massachusetts Subclass"). (*Id.* at ¶ 51.)

Plaintiff asserts four causes of action in her Complaint: (1) negligence; (2) breach of confidence; (3) breach of implied contract; and (4) breach of implied covenant of good faith and fair dealing. Based on these claims, she seeks various forms of equitable relief, damages, attorneys' fees, injunctive relief, and costs, among other forms of relief. (*Id.*, Prayer for Relief.)

III. PLEADING REQUIREMENTS

To survive a motion under Rule 12(B)(6), "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A litigant's claim has "facial plausibility" when he or she "pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* "Plausibility is the key, as the well-plead allegations must nudge the claim across the line from

conceivable to plausible." *Schatz v. Republican State Leadership Comm.*, 669 F.3d 50, 58 (1st Cir. 2012) (internal citations and quotations omitted). Thus, to satisfy this pleading standard, a complaint must offer more than "labels and conclusions or a formulaic recitation of the elements of a cause of action." *Twombly*, 550 U.S. at 555.

IV. ARGUMENT

Each of Plaintiff's claims fail as a matter of law. Each is addressed in turn.

A. Count I For Negligence Fails To Allege The Breach And Damages Elements Of The Claim.

To state a negligence claim, a plaintiff must plead duty, breach, causation, and damages. *See Jupin v. Kask*, 849 N.E.2d 829, 834-35 (Mass. 2006). In this case, Plaintiff fails to allege: (1) a breach by Cohen Cleary; and (2) cognizable damages.

1. Plaintiff fails to allege the breach of any relevant duty.

Federal pleading standards require that a complaint contain sufficient factual matter to state a claim that is plausible on its face and to allow the court to draw the reasonable inference that the defendant is liable for the alleged conduct. *Iqbal*, 556 U.S. at 678. Consistent with this standard, in the data-breach context, a plaintiff must allege facts – not labels and conclusions – describing the steps that the defendant could have or should have taken to prevent the incident. *E.g., Anderson v. Kimpton Hotel & Rest. Group, LLC*, No 19-cv-01860, 2019 WL 3753308, at *4-9 (N.D. Cal. Aug. 8, 2019) (dismissing data breach claims where plaintiffs failed to "plead any facts to support [their] conclusory assertions" related to defendant's supposedly inadequate cybersecurity measures); *cf. Springmeyer v. Marriott Int'l, Inc.*, No. 20-cv-867-PWG, 2021 WL 809894, at *3 (D. Md. Mar. 3, 2021) (dismissing claims for lack of standing where plaintiffs did not allege facts about what the defendant did wrong, how its cybersecurity was inadequate, how it failed to detect the attack, or why its breach notifications were untimely and inaccurate). Such is the case here.

Plaintiff contends that Cohen Cleary failed: "to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII in its possession" (Compl., ¶ 64); "to protect Representative Plaintiff's and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices" (*id.*); "to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches" (*id.*); and "to promptly notify Representative Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected its PHI/PII (*id.*), among other duties. Plaintiff, however, fails to cite any factual basis for her bare conclusions.

By way of examples, Plaintiff does not identify: (a) any particular industry standard or protocol that Cohen Cleary failed to adopt; (b) any legally significant way in which Cohen Cleary's notification of the Cyberattack to affected individuals was untimely or inaccurate; (c) how any of Cohen Cleary's security practices were inadequate or deficient; or (d) how Cohen Cleary failed to "adequately train" its employees (*see id.*, ¶ 72).

Plaintiff attempts to add some substance to her contentions in paragraphs 32 through 35, which purport to identify security measures Cohen Cleary should have implemented. But these allegations are merely a list of generic steps that a party may take to defend PII and these allegations do not outline with any specificity how Cohen Cleary may have failed to meet these steps, and merely presumes that Cohen Cleary failed to implement security measures because of the Cyberattack's occurrence. In other words, Plaintiff's allegations do not identify any particular failures or faults by Cohen Cleary. Like the plaintiffs in *Anderson* and *Springmeyer*, Plaintiff has not alleged any facts concerning what Cohen Cleary could or should have done to better protect

her information, how Cohen Cleary's security measures were insufficient, or in what way its response to the Cyberattack was untimely.

Plaintiff's threadbare allegations confirm that she is, in actuality, asking the Court to infer the breach of a duty from the mere existence of the Cyberattack. The law requires more than Plaintiff's general regurgitation surrounding general data security measures. Plaintiff must plausibly allege, with facts, how Cohen Cleary's specific conduct breached its purported duty to protect her information. She has not met this burden, and as such, she fails to state a claim for negligence.

2. Plaintiff cannot utilize negligence per se to establish the duty and breach elements.

Plaintiff claims that Cohen Cleary has failed to comply with 15 U.S.C. § 45, Sec. 5 (the "FTCA") by "failing to use reasonable measures to protect [her] PHI/PII. (Compl., ¶ 81-83.) Plaintiff, in effect, is attempting to rely on the FTCA to establish the standard of care necessary to plead the duty and breach elements of her negligence claim. As Massachusetts courts have long held, violation of a statute "is only some evidence of the defendant's negligence as to all consequences the statute was intended to prevent." *Bennett v. Eagle Brook Cnty Store, Inc.*, 408 Mass. 355, 358, 59 (1990).

Neither Massachusetts appellate courts, nor the First Circuit when applying Massachusetts law, have held that a plaintiff may rely on the FTCA when seeking to establish the standard of care in the data breach or cyberattack context. Accordingly, Cohen Cleary submits to this Court that Plaintiff may not rely on the FTCA herein because she has failed to allege facts demonstrating Cohen Cleary's purported failure to comply with the statute. Instead, Plaintiff asserts conclusory allegations that do not identify which of the FTCA's protocols are practices Defendant has failed to comply with. (*See id.* ¶¶81-83.) By way of example, Plaintiff contends that "Defendant [has

failed] to use 'reasonable measures' to protect PHI/PII" (*id.* ¶ 81) and that Defendant has not complied "with applicable industry standards" (*id.* ¶ 82.), but fails to identify the particular failures or faults specific to Cohen Cleary's security practices. These allegations fall short of the pleading standards required of her at this phase, and as such, her claim should be dismissed accordingly.

3. Plaintiff fails to allege legally cognizable damages.

Damages are an essential element of a negligence claim and alleging a "measurable loss" is "necessary" to establishing this element. *Portier v. NEO Tech. Solutions*, No. 3:17-cv-30111-TSH, 2019 WL 7946103, at *14-16 (D. Mass. Dec. 31, 2019) (citing *In re: SuperValu, Inc., Customer Data Sec. Breach Litig.*, Court File No. 14-MD-2586 ADM/TNL, 2018 WL 1189327, at *11 (D. Minn. Mar. 7, 2018), *aff'd sub nom. In re: SuperValu, Inc.*, 925 F.3d at 955 ("Data breach cases in Illinois and elsewhere have repeatedly held that a cardholder's mere allegation of an unauthorized charge, unaccompanied by an out-of-pocket loss, is not sufficient to state an actionable injury."). Thus, a plaintiff is required to plead facts giving rise to actual or cognizable damages because "[d]amages is the word which expresses in dollars and cents the injury sustained by a plaintiff." *Donovan v. Philip Morris USA, Inc.*, 914 N.E.2d 891, 899 (Mass. 2009) (internal citations and quotations omitted)).

Portier is instructive here. In *Portier*, the District of Massachusetts found that the representative plaintiffs in a data breach/cyberattack class action had *properly* pled the damages element of their negligence claim because they had alleged that an unauthorized third party had improperly used their PII after the occurrence of a cyberattack. 2019 WL 7946103, at *14-15. However, had plaintiffs not pled actual misuse of their data, or if they had failed to plead the actual monetary out of pocket expenses incurred when dealing with the aftermath of the cyberattack, then plaintiffs would not have been able to meet the "measureable loss" required of Massachusetts law

to adequately seek damages, which would have resulted in their failure to properly allege damages. *Id.* at *15-16.

Fraudulent misuse of a person's PII aside, other states, when opining on similar negligence and damages related issues in the cyberattack context, offer persuasive insight regarding the need for a plaintiff to allege actual and cognizable damages when stating a claim for negligence. *See Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14-1152RSL, WL 4940371 (W.D. Wash. Mar. 27, 2015). In *Lovell*, a plaintiff alleged that a restaurant, P.F. Chang's, failed to utilize industry standard cybersecurity practices, thereby allowing hackers to access his credit and debit card information. *Id.* at *1. The plaintiff further alleged that that he would have to "take steps" to protect himself, including joining credit fraud watch lists, and that these steps are "long, costly, and frustrating." *Id*. The plaintiff also claimed that he would be subjected to harassment and stalking as a result of the breach. *Id*.

Rejecting these claims, the court held that there was no indication that plaintiff had suffered any appreciable harm, and "[t]he mere danger of future harm, unaccompanied by present damage, will not support a negligence action." *Id* at *2 (citing *Krottner v. Starbucks Corp.*, 406 Fed. Appx 129, 131 (9th Cir. 2010)). The *Lovell* court further held that "[t]he fear that something might happen in the future is simply too speculative an injury to give rise to a present cause of action." *Id.* at *2.

Plaintiff claims to have suffered a variety of injuries due to the Cyberattack, from "lost time, annoyance, interference, and inconvenience," to "anxiety and increased concerns for the loss of privacy." (Compl., ¶ 12.) She also claims to suffer from a myriad of abstract and ill-supported injuries, such as the risk of identity theft and the purported "diminution in the value" of her PII. (*Id.*). None of these injuries, however, demonstrate the actual or measurable loss required of her

when pleading a claim for negligence. Furthermore, Plaintiff does not contend that her PII has been misused, whether fraudulently or otherwise, since the Cyberattack's occurrence.

As the *Portier* court highlighted, the actual misuse of a plaintiff's PII, in addition to facts alleging that a plaintiff has incurred out of pocket expenses associated with the aftermath of a cyberattack, are ways in which a plaintiff can positively demonstrate the existence of monetary damages within the data breach context. Plaintiff alleges no such actual, cognizable, or monetary damages in her Complaint. In addition, her fear of the *possible* misuse of her PII is baseless and unsupported. She does not allege that her PII has been accessed by any third-party individual, she does not allege that her PII is accessible anywhere on the internet or otherwise, and further fails to allege that her information has been bought or sold. In addition, Plaintiff fails to allege that she has incurred any actual costs as a direct result of the Cyberattack, and instead, flatly asserts that she has incurred "out-of-pocket" expenses with no specificity.

This Court should dismiss Plaintiff's negligence claim because she has failed to allege facts that, when construed as true, demonstrate any actual, cognizable, or monetary damages. The speculative risks of a 'future' harm are insufficient for pleading a claim for damages in the data breach context, especially when this risk is not imminent. As such, Plaintiff's Count I must be dismissed as a matter of law.

B. Count II For Breach Of Confidence Fails Because Plaintiff Fails To Allege That Defendant Voluntarily Or Affirmatively Disclosed Her PII.

Count II of Plaintiff's Complaint alleges that, by providing her PII to Cohen Cleary for services, the parties established both an explicit and implicit understanding that Cohen Cleary would "take precautions to protect" her PII from "unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing." (Compl., ¶ 91.) In other words, she claims that Cohen Cleary agreed to protect her PII in confidence, and that Cohen Cleary

breached this confidence by falling victim to the Cyberattack. To state a claim for breach of confidence, a plaintiff must allege that a defendant has a confidential relationship with the defendant, and that the defendant has engaged in the unprivileged use or disclosure of his or her information or secrets. *See Shaoguang Li v. Off. Of Transcription Serv's*, 63 N.E.3d 64 (Mass. App. Ct. 2016); *see also Burten v. Milton Bradley Co.*, 763 F.2d 461, 463 (1st Cir. 1985).

Massachusetts courts have yet to consider a claim for breach of confidence within the data breach or cyberattack context. Federal courts in other states, however, have dismissed breach of confidence claims. *Farmer v. Humana Inc.*, 582 F. Supp. 3d 1176, 1188-89 (M.D. Fla. 2022); *see Puris v. Aveanna Healthcare, LLC*, 563 F. Supp. 3d 1360, 1378 (N.D. Ga. 2021) ("Plaintiffs maintain that their breach of confidence claim should survive because they have alleged that Defendant (1) allowed the disclosure to happen and (2) failed to heed warnings that its records might be targeted in a cyberattack . . . [t]his argument is unavailing . . . [because the defendant's] inadequate security facilitated the theft, such a claim would lie in negligence not breach of confidence." (internal citations and quotations omitted). Expanding on this, courts have expressly found that a defendant cannot have improperly shared a plaintiff's confidential information when the information was stolen as a result of a cyberattack. *See Puris*, 563 F. Supp. 3d at 1378 (citing *In re Brinker Data Incident Litig.*, 3:18-cv-686-J-32MCR, 2020 WL 691848 (M.D. Fla. Jan. 27, 2020)).

In *Puris*, a pediatric home-care provider fell victim to a cyberattack, which resulted in the compromising of both patient and employee personal information. *Id.* at 1365. The *Puris* plaintiffs raised a claim for breach of confidence against the defendant, claiming that defendant engaged in the unprivileged disclosure of their information to third parties by falling victim to the cyberattack and by failing to take reasonable steps to present the attack. *Id.* at 1378. Rejecting this argument,

the court held that the plaintiff failed to allege facts demonstrating that defendant "disclosed" their PII, finding that "defendant did not do any act that made [p]laintiffs' information known—the information was stolen by third-parties." *Id.*

In the case at bar, Plaintiff fails to allege that Cohen Cleary voluntarily disclosed this information and expressly acknowledges that her information has been "placed in the hands of unauthorized third parties/criminals" who "infiltrated" Cohen Cleary's network servers. (Compl., ¶¶ 2, 12.) Plaintiff's own narrative establishes that Cohen Cleary did not intentionally disclose her PII and further establishes that Cohen Cleary did not engage in an affirmative act that resulted in the disclosure of her PII. Plaintiff's breach of confidence claim lacks merit and should be dismissed.

C. Count III For Breach Of Implied Contract Fails To Allege The Elements Of Contract Formation and Damages.

Plaintiff was a client of Defendant, a law firm, and she engaged it to provide her legal services. (*Id*. ¶¶ 7, 14.) But in Count III, Plaintiff alleges that she entered into an implied contract with Defendant for the safeguarding of her PII. (*Id*. ¶¶ 99, 102.) To state a claim for breach of contract, Plaintiff must plead: "(1) an agreement was made between the plaintiffs and the defendant supported by valid consideration; (2) the plaintiffs have been ready, willing, and able to perform; (3) the defendant's breach has prevented them from performing; and (4) the plaintiffs have suffered damage." *Hoang v. Eternal Salon, Inc.*, No. 16-P-812, 2017 WL 888387, at *1 (Mass. App. Ct. Mar. 6, 2017) (citing *Singarella v. Boston*, 342 Mass. 385, 387 (1961). "In the absence of an express agreement, an implied contract may be found to exist from the conduct and relations of the parties." *Anisgard v. Bray*, 419 N.E.2d 315, 318 (Mass. App. Ct. 1981) (internal citations and quotations omitted). Plaintiff, here, fails to allege the first and fourth elements of the claim.

1. Plaintiff fails to allege the existence of consideration.

To plead and prove consideration, "the contract must be a bargained-for exchange in which there is a legal detriment of the promise or a corresponding benefit to the promisor." *Neuhoff v. Marvin Lumber and Cedar Co.*, 370 F.3d 197, 201 (1st Cir. 2004). Plaintiff does not allege that she provided any bargained-for exchange of legal value or detriment to Defendant for the safeguarding of her PII from cyber criminals. She fails to allege that she provided any consideration at all for the purported implied contract she is attempting to enforce.

Plaintiff alleges that as a part of the supposed contract, Cohen Cleary promised to safeguard and protect her information, and to timely and accurately notify her of any compromise of it (*id.* ¶ 102, 105). But Plaintiff also alleges that Cohen Cleary's supposed duty arising out of this "contract" was "independent" and "untethered to any contract" between the parties. (*Id.* ¶ 71.) Thus, Plaintiff fails to establish what consideration was provided in exchange for the digital protection of her PII from cyber attackers, and as such, her claim fails as a matter of law.

2. Plaintiff fails to allege mutual assent.

Contract formation "requires a bargain in which there is a manifestation of mutual assent to the exchange." *Vacca v. Bringham & Women's Hosp., Inc.*, 156 N.E.3d 800, 806 (Mass. App. Ct. 2020) (internal citations and quotations omitted). A meeting of the minds "occurs when there is an offer by one [party] and an acceptance of it by the other." *Id.* Critically, this offer "is a manifestation of willingness to enter into a bargain, so made as to justify another person in understanding that his assent to that bargain is invited and will conclude it." *Id.*

Here, Plaintiff's Complaint is devoid of allegations concerning the parties' supposed mutual assent to contractual terms pertaining to the protection of her PII from cyber attackers. Nowhere does Plaintiff allege the terms of the purported implied contract, much less the conduct,

language, or other pertinent circumstances from which an agreement to be bound can be inferred. Instead, the most she can muster is the *conclusion* – unsupported by any fact – that, upon providing her PII to Cohen Cleary as a condition to receiving legal services, that the parties then agreed "amongst other things" to the "protection of [her] PHI/PII." (Compl., ¶ 103.) This is the full extent of Plaintiff's allegations of a "meeting of the minds" and it falls far short of alleging mutual assent. Absent allegations that the parties discussed, understood, or were even aware of the necessary terms, i.e., safeguarding her PII, Plaintiff has not alleged that the Parties reached a meeting of the minds on any contract.

3. Plaintiff fails to allege legally cognizable damages.

Under Massachusetts's law, a plaintiff asserting a breach of contract claim must show damages. *See Scholz v. Goudreau*, 901 F.3d 37, 43 (1st Cir. 2018). Plaintiff's claims for "damages" are not actual, present, or cognizable. (See infra, §IV(A)(2).) Accordingly, Plaintiff cannot demonstrate what type of damages – if any – have resulted from the alleged Cyberattack and her claim for breach of implied contract must be dismissed.

D. Count IV For Breach Of Implied Covenant Of Good Faith And Fair Dealing Fails Because It Is Duplicitous.

Under Massachusetts law, a covenant of good faith and fair dealing is "implied in every contract." *Zoll Med. Corp. v. Barracuda Networks, Inc.*, 585 F. Supp. 3d 128, 138 (D. Mass. 2022) (citing *Uno Rests v. Boston Kenmore Realty Corp.*, 441 Mass. 376 (2004)). "While it is true that every Massachusetts contract carries with it an implied covenant of good faith and fair dealing, a breach of the implied covenant does not give rise to a cause of action independent of the underlying contract." *Med. Source, Inc. v. PerkinElemer Health Sciences, Inc.*, No. 1684CV01853BLS1, 2020 WL 960592, at *3 (Mass. Super. Ct. Jan. 9, 2020) (citing *Mill-Bern Assocs., Inc. v. Dallas Semiconductor Corp.*, No. 98-1435-D, 2002 WL 1340853, at *9 (Mass. Super. Ct. June 13, 2002),

aff'd, 799 N.E.2d 606 (Mass. App. Ct. 2003)). [R]ather, a claim for breach of the implied covenant is, in substance, a claim of breach of contract[.]" *Shepherd Kaplan Krochuk, LLC v. Borzilleri*, No. 1884CV01418BLS1, 2018 WL 7246977, at *4 (Mass. Super. Ct. Dec. 7, 2018) (citing *Mill-Bern Assocs.*, 2002 WL 1340853, at *9, *aff'd* 799 N.E.2d 606 (Mass. App. Ct. 2003).

In her final cause of action, Plaintiff asserts a claim for breach of implied covenant of good faith and fair dealing independent of her breach of contract claim, Count III. She alleges that Cohen Cleary breached this implied covenant by "failing to maintain adequate computer systems and data security practices to safeguard" her PII and by failing to timely notify her of the Cyberattack. (*Id.* ¶ 110.) Plaintiff further accuses Cohen Cleary of denying her "the full benefit of the[] bargain" in Cohen Cleary's purported failure to protect her PII from cyber attackers and in failing to maintain adequate security measures. (*Id.* ¶ 111.) To the extent Plaintiff can state a claim for breach of an implied contract with Cohen Cleary, then Count IV is subsumed by Count III. If she cannot state a claim for breach of implied contract, then Count IV cannot stand alone. Either way, Plaintiff cannot state an independent claim for breach of the implied covenant of good faith and fair dealing and Count IV must be dismissed.

V. CONCLUSION

For the foregoing reasons, Defendant Cohen Cleary respectfully requests that the Court: (A) grant this Motion in its entirety and dismiss Plaintiff's Complaint; and (B) award Cohen Cleary such other and further relief as is appropriate.

Respectfully submitted,

/s/ Lindsey A. Gil

Jennifer E. Burke, BBO# 554632
Lindsey A. Gil, BBO# 679626
Peabody & Arnold LLP

600 Atlantic Avenue
Boston, MA 02210
T: 617.951.2004
F: 617.235.3550
jburke@peabodyarnold.com
lgil@peabodyarnold.com

Timothy J. Lowe (*pro hac vice application forthcoming*)
McDonald Hopkins
39533 Woodward Avenue, Suite 318
Bloomfield Hills
MI 48304
tlowe@mcdonaldhopkins.com

Counsel for Defendant

Dated: May 15, 2023

CERTIFICATE OF SERVICE

I hereby certify that on May 15, 2023, I electronically filed the foregoing document using the electronic filing system, which will send notification of such filing to all attorneys of record.

Respectfully submitted,

/s/ Lindsey A. Gil

Lindsey A. Gil

2519669